Mathematics 6310
Assignment 9, due November 7, 2011

Read 12.1. Then do the following:

- 12.1 (pp. 468–472): 2, 10, 11, 12 [There's a typo in 10 (missing hypothesis).]

Additional problems.

1. This exercise fills in the details of the theory of algebraic independence that I sketched in class. A good old-fashioned reference for this is van der Waerden, pp. 99–103 and 200–202. You are welcome (and even encouraged) to read this, but please write the proofs in your own words and with modern notation. Let K/F be a field extension. Recall that $\alpha_1, \dots, \alpha_n \in K$ are *algebraically independent* over F if they satisfy no polynomial equation $f(\alpha_1, \dots, \alpha_n) = 0$ with $f \neq 0$ in $F[x_1, \dots, x_n]$. And $\beta \in K$ is said to *depend algebraically* on elements $\alpha_1, \dots, \alpha_n$ (which are not necessarily independent) if β is algebraic over $F(\alpha_1, \dots, \alpha_n)$. I will often omit the word "algebraically" below. Prove the following:
   (a) $\alpha_1, \dots, \alpha_n$ are independent if and only if no α_i depends on the set of α_j with $j \neq i$.
   (b) If β depends on $\alpha_1, \dots, \alpha_n$ but not on $\alpha_1, \dots, \alpha_{n-1}$, then α_n depends on $\alpha_1, \dots, \alpha_{n-1}, \beta$.
   (c) If γ depends on $\beta_1, \dots, \beta_k$ and each β_i depends on $\alpha_1, \dots, \alpha_n$, then γ depends on $\alpha_1, \dots, \alpha_n$.
   (d) (*Exchange property*, or *replacement property*) Let A and B be (finite) subsets of K such that A is independent and each $\alpha \in A$ depends on B. Then there is a subset $A' \subseteq B$ with $|A'| = |A|$ such that $(B \smallsetminus A') \cup A$ is equivalent to B (i.e., everything in one set depends on the other set).
   (e) Two equivalent independent sets have the same number of elements.
   (f) If K is finitely generated over F, then any set of generators has an algebraically independent subset $\alpha_1, \dots, \alpha_n$ such that K is a finite extension of $F(\alpha_1, \dots, \alpha_n)$. The number n, called the *transcendence degree* of K over F, is well defined (i.e., independent of the choices).

2. Exercise 12.1.2 implies, in particular, that every integral domain R has the *invariant basis number* property (IBN), i.e., if F is a finitely-generated free R-module, then all bases of F have the same size. Equivalently, if $R^n \cong R^m$, then $n = m$. [I actually used this tacitly a couple times in the proof of the stacked basis theorem.] This generalizes a familiar property of vector spaces. In the present exercise you will generalize the IBN property to a larger class of rings than integral domains. [Note: It does *not* hold for arbitrary rings.]
   (a) If R is a ring (not necessarily commutative) that admits a homomorphism to a field, then R has the IBN property.
   (b) More generally, if R admits a homomorphism to a commutative ring in which $1 \neq 0$, then R has the IBN property.

3. Let R be a PID. The proof of the structure theorem for finitely-generated R-modules given in class (and in the text) is nonconstructive at the point where one has to pick a maximal element from a collection of ideals. If R is a Euclidean domain, however, such as $\mathbb{Z}$ or $F[x]$, the proof can be done in a more concrete,

constructive way. This is outlined in Exercises 16–19 in Section 12.1. Read through those exercises to see the method, and then use the method to analyze the structure of the abelian group ($\mathbb{Z}$-module) M with three generators x, y, z and the following three defining relations:

$$\begin{aligned} 2x + 2y + 14z &= 0 \\ 2x + 4y + \ \ 2z &= 0 \\ 5z + 5y + 29z &= 0. \end{aligned}$$

This means, by definition, that M is the quotient of $\mathbb{Z}^3$ by the subgroup generated by $(2, 2, 14)$, $(2, 4, 2)$, and $(5, 5, 29)$.